

ABSTRACT

Methods, systems, and computer program products are disclosed for protecting the security of resources in distributed computing environments. The disclosed techniques improve administration and enforcement of security policies. Allowed actions on resources, also called permissions, (such as invocations of particular methods, read or write access of a particular row or perhaps a particular column in a database table, and so forth) are grouped, and each group of permissions is associated with a role name. A particular action on a particular resource may be specified in more than one group, and therefore may be associated with more than one role. Each role is administered as a security object. Users and/or user groups may be associated with one or more roles. At run-time, access to a resource is protected by determining whether the invoking user has been associated with (granted) at least one of the roles required for this type of access on this resource.